HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

Standing Committee on Access to Information, Privacy and Ethics

ETHI • NUMBER 030 • 1st SESSION • 42nd PARLIAMENT

EVIDENCE

Tuesday, October 25, 2016

Chair

Mr. Blaine Calkins

Standing Committee on Access to Information, Privacy and Ethics

Tuesday, October 25, 2016

● (1110)

[*English*]

The Chair (Mr. Blaine Calkins (Red Deer—Lacombe, CPC)): Good morning, everyone.

Good morning to our witnesses. Thank you very much for your patience as we had to consider a vote in the House of Commons. We're only a few minutes behind, so I appreciate colleagues getting here as quickly as possible.

We're continuing on with our study of the Privacy Act. We're pleased to have with us representatives from the Canada Border Services Agency, the RCMP, the Canadian Security Intelligence Service, and the Department of Citizenship and Immigration. The list of names is long, and I'll let each of you introduce yourself at the start. We'll allow 10 minutes of opening comments for each department, so you can decide how you want to use that time accordingly.

We thank you very much for being here today. I ask you to be succinct, within that 10 minutes, and then we can get to the rounds of questioning. You all know how this works. I think all of you have been before a committee before. I'm looking forward to this.

I'll just go in the order you appear here on my agenda. We'll start with the Canada Border Services Agency for up to 10 minutes, please.

Mr. Robert Mundie (Director General, Corporate Secretariat, Canada Border Services Agency): Thank you, Mr. Chair.

My name is Robert Mundie. I'm the director general of the corporate secretariat at the Canada Border Services Agency. I am also the chief privacy officer for CBSA. I have with me Mr. Dan Proulx, who is the director of our ATIP division.

The ATIP division is responsible for oversight of the privacy function at the agency, which includes administering and fulfilling all legislative requirements of the Privacy Act related to the processing of requests; interacting with the public, CBSA employees, other government institutions, and the Office of the Privacy Commissioner regarding investigations and audits; and implementing measures to enhance our capacity to process privacy requests.

I will briefly outline the CBSA's privacy function and the way the agency performs against established service standards, and I'll highlight some of the successes and challenges we experience in our administration of the act.

[*Translation*]

The Canada Border Services Agency is responsible for border functions related to customs; the enforcement of the Immigration and Refugee Protection Act; and food, plant and animal inspection.

The agency administers and enforces two principal pieces of legislation. First, the Customs Act outlines the agency's responsibilities to collect duties and taxes on imported goods, interdict illegal goods, and administer trade legislation and agreements. Second, the Immigration and Refugee Protection Act governs both the admissibility of people into Canada, and the identification, detention and removal of those deemed to be inadmissible under the act.

[*English*]

The agency also enforces over 90 other statutes on behalf of other federal government departments and agencies.

Mr. Chair, given the numerous daily interactions that the agency has with businesses and with individuals on a variety of matters, we are no strangers to privacy requests. Approximately 60 employees work in the ATIP division, 34 of whom are dedicated to the processing of privacy and access to information requests. The division also has an internal network. It works with 16 liaison officers who provide support across the agency's branches at headquarters and in the regions in fulfillment of access and privacy requests.

The CBSA's operating expenditures to run its program for privacy and access totalled approximately $5.4 million in the previous fiscal year, with $4.4 million dedicated to salary and $1 million to non-salary expenditures. This amount includes the costs of administering both the Access to Information Act and the Privacy Act, as work on both acts is done concurrently.

With respect to volumes, the CBSA received just over 11,200 requests in the previous fiscal year, 2015-16, the second-highest number within the Government of Canada. In addition to these, the agency received approximately 5,500 access to information requests.

The high volumes are largely attributable to individuals seeking copies of their history of arrival dates into Canada. In 2015-16, 78% of all the requests that came to the CBSA were from individuals seeking their traveller history report, which is used to support residency requirements for programs administered by Immigration, Refugees and Citizenship Canada and by Employment and Social Development Canada. Of all the requests completed, the CBSA was successful in responding to 88.7% of them within the legislated timelines in the previous fiscal year.

ATI analysts in case-processing units have direct access to the database that houses the traveller history reports, and the review of these reports and the application of law are relatively standard, which allows them to complete these requests without needing to obtain recommendations on disclosure from departmental officials. This greatly reduces the time it takes analysts to process these types of requests.

[*Translation*]

As indicated in the Office of the Privacy Commissioner of Canada's 2015-16 annual report to Parliament, 88 complaints were filed against the CBSA to the Privacy Commissioner of Canada. Given the large volume of requests the agency processes, this number is a very small proportion of the total requests closed.

However, we always aspire to better serve the requesters. Our successes reflect the agency's commitment to ensuring that every reasonable effort is made to meet obligations under the Privacy Act.

[*English*]

The CBSA strives to provide Canadians with the information to which they have a right in a timely and helpful manner, by balancing the right of access with the need to protect the integrity of border services that support national security and public safety. We take our responsibilities under the Privacy Act very seriously.

In closing, we welcome the review of the Privacy Act, and will fully support and adopt any measures that are introduced by the Treasury Board Secretariat in response to changes made to the act.

I want to thank you, Mr. Chair, for the opportunity to provide our input into your study, and for welcoming us here today. I look forward to questions members of the committee may have.

● (1115)

The Chair: Thank you very much, Mr. Mundie, it's great to have you at committee.

We'll move to the Royal Canadian Mounted Police, for 10 minutes please.

Ms. Marcoux.

Ms. Rennie Marcoux (Chief Strategic Policy and Planning Officer, Royal Canadian Mounted Police): Thank you, Mr. Chair, for the opportunity to appear before this committee to assist in your review of the Privacy Act.

This is an important review, given the profound changes in society, and the security landscape changes since the Privacy Act came into force in 1983. The RCMP welcomes this review and is committed to working with all government departments and agencies in considering changes to the act that balance privacy in an environment driven by constantly evolving information technology.

My name is Rennie Marcoux and I am the chief strategic policy and planning officer responsible for the access to information and privacy branch at the RCMP. I am accompanied by my colleague, assistant commissioner Joe Oliver, who is responsible for technical operations.

[*Translation*]

I will begin by describing how the RCMP is structured to respond to privacy requests. Then, I will explain some of the measures we have in place to promote compliance with the Privacy Act. Lastly, I will close with a few words on the importance of information in fulfilling our mandate.

[*English*]

The RCMP is divided into 15 divisions plus the national headquarters in Ottawa, each of which is under the direction of a commanding officer. At the local level, there are more than 750 detachments.

Given the size of our organization, the diversity and complexity of our operations, and the sensitive nature of our information holdings, responding to Access to Information and Privacy Act requests imposes a significant demand on the organization. Notably, we must be very careful in the collection, use, and disclosure of personal information in accordance with the Privacy Act.

[*Translation*]

The access to information and privacy branch at the RCMP is responsible for responding to all formal requests for information under the two acts. In addition, the access to information and privacy branch develops policies and procedures for use within the RCMP to ensure compliance with the legislation, regulations and associated guidelines.

[*English*]

We have approximately 68 employees, whose main focus of work is meeting the RCMP's obligations under the act. A quarter of these positions require police officers to ensure sensitive law enforcement information is properly protected, and to reduce the need for time-consuming consultations with our program managers. The employees are required to work with approximately 750 points of contact in our divisions across Canada.

The ATIP branch is responsible for coordinating the retrieval and release of records for the entire organization. The contacts in the divisions assist in identifying relevant records and ensuring that regional employees are aware of their responsibilities under the act.

In 2015-16, the RCMP received slightly over 5,000 Privacy Act requests, and our compliance rate was 82% compared to 78% from the previous year. For the first time since the fiscal year 2010-11, the RCMP was able to raise its compliance above the 80% standard set by the Office of the Privacy Commissioner.

[*Translation*]

The RCMP's overall performance improved last fiscal year, since we closed more files, reduced late responses, and received fewer complaints.

These results follow an organizational workload review that led to the restructuring of the access to information and privacy branch so that it could process access requests more efficiently at intake. These changes represent a positive step for the RCMP.

The RCMP is very careful to comply with the Privacy Act when releasing information. For example, information is released only with consent or only to individuals and institutions authorized to receive the information. When disclosing personal information, the RCMP ensures that it has the disclosure authority under the act and that the requesting or recipient agency has the proper statutory authority.

● (1120)

In disclosures of personal information deemed to be of public interest, apart from a few senior officials at headquarters, only the commanding officers are authorized to make the decision.

[*English*]

As part of the ATIP branch's initiative to educate all RCMP employees, 21 presentations explaining their responsibilities under the Privacy Act were given to more than 200 employees last year. The RCMP is developing enhanced privacy training tools for all employees and reviewed its policies and definitions relating to personal information, including guidance around the release of information in the public interest.

[*Translation*]

An access to information and privacy training plan has been developed and implemented. Access to information and privacy personnel are regularly attending sessions provided by the Treasury Board Secretariat as well as other training sessions and workshops as part of their development.

The training strategy encourages the employees to enrol in various access to information and privacy-related courses as a way to gain knowledge and improve their efficiency as specialists in the field.

As a part of their orientation, all employees receive five days of training on the two acts when they arrive in the branch.

We're also focusing on training at the detachment level to ensure that frontline employees know the RCMP's obligations under the federal legislation.

[*English*]

The mandate of the RCMP is to prevent crime and apprehend offenders. The collection and sharing of information is essential to this mandate. The fast-paced transactional nature of crime requires that we act quickly and partner with other police forces and security agencies in Canada and around the world. Effective and responsible information sharing with our security partners has become increasingly essential to identify threats and protect public safety.

The RCMP enforces the laws of Canada in accordance with appropriate judicial authorization. We adhere to privacy standards set forth by the Government of Canada, and we're conscious of the need to take the utmost care when handling the sensitive or private information of suspects and victims.

[*Translation*]

We take our obligations under the Privacy Act very seriously and make every effort to balance those obligations with our main priority to ensure the security of Canadians.

[*English*]

Any review of the Privacy Act should continue to balance the need to protect the privacy rights of Canadians with the need for security agencies to have the appropriate authorities to investigate criminal activities and to protect the safety and security of Canadians.

[*Translation*]

Thank you again, Mr. Chair, for the opportunity to appear before the committee.

[*English*]

The Chair: Thank you, Ms. Marcoux. We very much appreciate that.

We'll now move on to CSIS, Mr. Michael Peirce, for up to 10 minutes, please.

Mr. Michael Peirce (Assistant Director Intelligence, Canadian Security Intelligence Service): Good morning, Mr. Chair and members of the committee.

I'm pleased to be here this morning before you, and with my colleagues.

My name is Michael Peirce. I am the assistant director of intelligence at CSIS. I am responsible for the production and dissemination of service intelligence. I am also responsible for matters pertaining to litigation and disclosure, including access to information and privacy.

I want to thank you for the invitation to be here today to contribute to your study of the Privacy Act, and for the opportunity to provide some insight into how CSIS manages privacy requests.

To begin, I would like to assure members that privacy and the protection of personal information are essential considerations for the service, both in its collection activities and in the information management policies and practices of our organization. Balancing transparency and accountability with our operational requirements is an ongoing effort that we respect and take seriously.

As is every other government institution, CSIS is subject to the Privacy Act. In that context, CSIS's mandate and operational activities create distinct requirements as they relate to privacy and access to information. That being said, and to contextualize my statements here today, I would like to provide members with a brief overview of CSIS's authorities and reasons that special consideration is required to protect the integrity of the work that we do.

CSIS's mandate is clearly defined in the CSIS Act. We are authorized to collect information only to the extent strictly necessary on activities suspected of constituting a threat to the security of Canada.

These threats are explicitly defined in section 2 of our act. They are limited to terrorism, espionage, sabotage, and foreign interference. In order to achieve our mission—that is, to protect national security—we collect this information to detect, assess, and respond to threats to the security of Canada. In terms of our response, we are specifically mandated to advise government on matters of national security, which can include sharing information with partners to inform their lawful investigations or their enforcement actions.

I would note, however, that CSIS itself is not an enforcement agency. We do not have the authority to arrest or detain individuals, nor do we enforce laws or make administrative decisions.

Because of our duties and functions, access to reliable and accurate information is the essence of what we do. CSIS understands its unique role in this regard and therefore strives to diligently manage and protect information it collects.

In this regard, Mr. Chair, in August 2015, the Security of Canada Information Sharing Act, or SCISA as I'll refer to it, entered into force, providing explicit authority for Government of Canada departments and agencies to share information with designated recipients in accordance with the relevant provisions of the act. CSIS is a designated recipient under this legislation.

To give effect to this legislation, CSIS is engaging with partners bilaterally, on a prioritized basis, to renew information-sharing relationships. This incremental approach has being adopted as a practical matter to ensure that relevant legal, policy, and privacy considerations are fully considered.

In fall 2015, CSIS presented its overall approach to the implementation of SCISA to officials at the Office of the Privacy Commissioner. Engagement is constructive and ongoing.

Now to return more specifically to the issue of privacy and access to information, I can tell members that CSIS devotes considerable efforts to addressing all mandatory reporting requirements under the Privacy Act, and we continue to maintain a high performance standard in its administration.

The service's ATIP section has 15 employees who fulfill the service's obligations under the Access to Information Act and Privacy Act, a relatively small number of resources, given the volume and complexity of the requests that we have, but they have demonstrated that they are up to the task.

During the 2015-16 fiscal year, CSIS received 1,212 requests under the Privacy Act alone, an increase of 149% over the previous year. Despite this—and I am rather proud to be able to tell you this—CSIS achieved an on-time completion rate of 99%.

CSIS is also one of 32 government institutions that accept online access to information requests, which has contributed to the increase in the number of requests that we receive.

I would also note that CSIS has a very productive relationship with the Office of the Privacy Commissioner in regard to complaints, and our ATIP section works diligently with the Office of the Privacy Commissioner to address every complaint that is filed.

● (1125)

As you are aware, the Privacy Act grants individuals the right to access their personal information. We diligently strive to balance the individual's right to access and our operational requirements to safeguard sensitive information pertaining to lawful investigations.

With respect to access to personal information, it is easy to appreciate why CSIS information requires some special consideration. It includes information on active national security investigations as well as information on investigative techniques that are unique to CSIS.

We also have to protect the personal safety of our employees and human sources who provide information to us. Of interest, there are a number of personal information banks that are unique to CSIS, including investigational records, security assessments, and advice.

The majority of Privacy Act requests to CSIS are for information contained in these banks. The investigational records bank, for instance, includes personal information on identifiable individuals whose activities are suspected of constituting threats to the security of Canada, and on identifiable individuals who are or were confidential sources of information. Clearly, these are records that must be protected.

While in principle this may seem straightforward, in practice it presents challenges. For example, we receive requests from individuals who are subjects of investigations, but also many more from individuals who are not and who have never been part of an investigation. Our policy is that we will neither confirm nor deny the existence of records in those circumstances. To do so would inadvertently confirm our investigative interests.

It should be noted that each privacy request is established and reviewed on a case-by-case basis. For each request, CSIS seeks to strike a balance that satisfies the legislated disclosure requirements and the need to protect matters of national security, public safety, and individual privacy.

I hope this usefully illustrates the balance that is achieved in fulfilling our obligations under the Privacy Act and our mandate under the CSIS Act. More broadly, all of CSIS' activities are pursued within a broad framework for accountability, both internally and externally. CSIS maintains an open relationship with the Privacy Commissioner, who is charged with overseeing compliance with the Privacy Act. Our activities are also subject to review by SIRC, the Security Intelligence Review Committee, which reports to Parliament on our operations.

I welcome the opportunity to appear before the committee today to discuss these matters, and with that, Mr. Chair, I will conclude my remarks.

● (1130)

The Chair: Thank you very much, Mr. Peirce. We'll now have our last witnesses from the Department of Citizenship and Immigration.

Ms. Beck, you're going to lead us off for up to 10 minutes, please.

[*Translation*]

Ms. Stefanie Beck (Assistant Deputy Minister, Corporate Services, Department of Citizenship and Immigration): Thank you.

[*English*]

Good morning, Mr. Chair and members. My name is Stefanie Beck. I am the assistant deputy minister of corporate services at Immigration, Refugees and Citizenship Canada.

[*Translation*]

I'm joined by Audrey White, the director of our access to information and privacy division.

[*English*]

We've been here before to talk about access to information, and we are very happy to be back to talk about privacy as well. Thank you very much for welcoming me and my colleagues here today. We're very happy to provide IRCC's input into this important matter.

We congratulate the committee on its study. It has been more than three decades since the Privacy Act came into play. I know we all agree it's time for an update. As the Privacy Commissioner has pointed out to this committee, developments in technology have made it possible to collect and retain enormous amounts of information. We must make sure that our ability to safeguard this information reflects this reality.

[*Translation*]

Mr. Chair, before I take questions from the committee, I would like to provide an overview of how Immigration, Refugees and Citizenship Canada deals with the challenges of protecting the personal information entrusted to it. It's a duty my colleagues and I take extremely seriously.

Our department has an access to information and privacy division with approximately 70 staff and a network of 85 liaison officers across the many branches and regions of the department.

Immigration, Refugees and Citizenship Canada receives more privacy requests than any other federal institution. In 2015-16, our most recent reporting year, we received 15,292 privacy requests. This year, we expect to receive over 16,000 requests.

I had the opportunity to appear before this committee earlier this year. Today, I will focus my comments on the Privacy Act.

[*English*]

Due to the nature of our work, which involves the processing of over 2.8 million applications for permanent and temporary residence every year, we receive an enormous amount of documentation containing personal information every day. This comes in every format—digital, print, and even photographs.

At IRCC, protecting privacy and personal information is paramount. The department has named a chief privacy officer to provide strategic leadership and direction on privacy. IRCC will hold its first annual privacy day next month. We plan to bolster privacy awareness and to champion the protection of personal information among staff. IRCC runs mandatory and voluntary online and in-person training activities such as workshops and awareness sessions. This is an ongoing process, not just once a year when it happens to be privacy day.

We have also adopted a widely disseminated privacy framework that promotes best practices for the handling of personal information all across the department. The privacy framework outlines key responsibilities and establishes a common set of standards and procedures. It identifies key privacy principles, such as limiting the collection, use, disclosure, and retention of information. The framework also provides employees with tools to ensure they are meeting their responsibilities and following the appropriate practices in line with Treasury Board Secretariat and departmental policies.

Just as a couple of examples, the privacy framework provides employees with information to ensure they are fully aware that personal information can be collected only as set out in IRCC's enabling legislation, primarily the Immigration and Refugee Protection Act, the Citizenship Act, and the Canadian Passport Order. It emphasizes that only employees with the appropriate security clearance should have access to personal information, and furthermore, that access to personal information should only be granted on a need-to-know basis. It's not sufficient just to have clearance, you have to need to know the information.

These principles that are at the heart of IRCC's privacy practices closely reflect many of the concerns raised by the Privacy Commissioner.

● (1135)

[*Translation*]

IRCC's privacy practices are in line with most of what is contained in the commissioner's recommendations for changes to the Privacy Act.

For example, as recommended by the commissioner, IRCC follows the Treasury Board Secretariat's policies, as well as its own privacy breach guidelines, which require all privacy breaches considered material in nature to be reported to the Privacy Commissioner and to the Treasury Board Secretariat.

The commissioner also recommends that government institutions be required to conduct privacy impact assessments for new or significantly amended programs, and to submit these assessments to the Office of the Privacy Commissioner before implementing the programs.

[*English*]

Again, Mr. Chair, this is something IRCC already does by following the privacy policies of the Treasury Board Secretariat and our own internal ones. Furthermore, in certain complex cases, IRCC officials will meet with the Privacy Commissioner's office to inform them in advance of the initiative and to provide a detailed briefing on potential impacts regarding privacy. We find that seeking feedback at an early stage enables us to develop better products.

These are just a couple of examples, Mr. Chair, of how the majority of the recommendations put forward by the Privacy Commissioner align with our practices for managing and handling personal information.

I should mention that there is one recommendation that could have a significant operational impact on our work. As you know, Mr. Chair, the Privacy Act currently affords access rights only to Canadian citizens, permanent residents, or people physically present in Canada. Currently, foreign nationals and those outside of Canada can obtain access to their personal information by hiring a Canadian representative and filing a request under the Access to Information Act. We discussed this the last time I was here, and as you know, they pay a fee when they make a request under the Access to Information Act.

[*Translation*]

The Privacy Commissioner has recommended that foreign nationals and those outside Canada should be able to submit a request for their personal information under the act. Our concern with this proposal is that, because of IRCC's lines of business and international mandate, the proposed recommendation could lead to an enormous increase in privacy requests that would place an undue burden on our resources and create considerable operational constraints. This could seriously compromise our ability to meet the deadlines for responding to requests as set out in the act.

Mr. Chair, I would like to thank you again for the invitation to provide IRCC's views on this important subject.

I'm happy to answer your questions.

[*English*]

The Chair: Thank you very much, Ms. Beck. We appreciate that.

We are going to proceed to our rounds of questioning.

I'll just remind my colleagues at the table that our questions should be eliciting responses pursuant to the study of the Privacy Act that we're undertaking right now.

[*Translation*]

Mr. Massé, you have seven minutes.

Mr. Rémi Massé (Avignon—La Mitis—Matane—Matapédia, Lib.): Thank you, Mr. Chair. Are you worried our questions won't be related to the specific field of the study? I'm kidding.

Thank you for being here this morning as witnesses. Your presence is greatly appreciated. This study is very important for the committee.

Thank you, Ms. Marcoux. You covered the essence of my question.

My question is for the four organizations. Please answer with a yes or no. I want to know whether all your employees receive training on their privacy responsibilities.

Mr. Robert Mundie: Yes.

Ms. Rennie Marcoux: Yes.

Mr. Michael Peirce: Yes, absolutely.

Ms. Stefanie Beck: Absolutely.

● (1140)

Mr. Rémi Massé: Thank you.

Given the complexity of your organizations, the number of employees in your organizations, the number of documents you develop and receive, and all your complex information systems, how can you ensure the personal information in those systems and documents is properly protected?

Obviously, the question is broad. It can be answered in one or two minutes.

In short, how can you confirm the personal information in your possession is properly protected?

We'll start with Mr. Mundie.

[*English*]

Mr. Robert Mundie: I'll start and then ask Mr. Proulx to add his comments.

The first thing, as you mentioned, is the training that's provided to our employees, so that there's an awareness of the act and how it applies to our operations. We have different types of training for different situations, from online to in-class to very specialized sessions for people who have particular functions within the organization. That's a key element.

Awareness is something that I support at the executive table and through different activities that are conducted on a regular basis. That's the awareness component.

We do a lot to prepare ourselves in terms of understanding the implications for privacy of different programs. We have privacy impact assessments that are prepared and occasionally refreshed, depending on changes in our environment in the program. We do consultations with the Office of the Privacy Commission on those. We have a clear understanding of what the implications are for us. We have mitigation measures that we can put in place whereby we identify potential risks to privacy due to our operations. Those are a couple of things that I would identify.

Dan, is there anything else you want to add?

Mr. Dan Proulx (Director, Access to Information and Privacy Division, Canada Border Services Agency): I would add that our agency records are always properly classified and properly designated.

We have a departmental security officer who we follow regarding the strict security requirements on the safeguarding of the information. We have an IT infrastructure that keeps all of that intact.

The same applies to my ATIP office. It's all on a need-to-know basis. We make sure that the information we retain is accurate and up to date and that it is treated according to its designation and classification.

Thank you.

[*Translation*]

Ms. Rennie Marcoux: I'll answer part of the question and then I'll turn the floor over to my colleague, if you don't mind.

As mentioned by my colleagues from the agency, our employees receive ongoing training and in-depth training. Privacy policies are in place. The employees responsible for access to information and privacy work closely with the staff in charge of information management in the RCMP. There is also information technology and oversight mechanisms implemented by the Privacy Commissioner. The duty to report privacy breaches creates a certain level of discipline and awareness in the organization. Lastly, the Office of the Privacy Commissioner regularly audits our information.

I'll now turn the floor over to Mr. Oliver.

Assistant Commissioner Joe Oliver (Assistant Commissioner, Technical Operations, Royal Canadian Mounted Police): Thank you, Ms. Marcoux.

I'll answer in English.

[*English*]

When it comes to the protection of information, we also follow the government's policy on security, which that includes a suite of policies on things such as physical security controls, personnel security controls, and IT security. When I talk about physical security, that could mean high-security areas where there's sensitive information. Only certain individuals will have access, so there's restricted access into high-security zones. When it comes to individual access, people are security cleared to a certain level. There are security controls in terms of the reliability of individuals to access information and the need to know and the right to know. The IT systems are also configured in such a way that certain individuals will only have access to certain information. For instance, in our National Sex Offender Registry, it's only those individuals within the national sex offender program who are designated who can access that information, not everybody in the RCMP.

There are administrative controls put on our security systems, as well as built-in controls to prevent cyber-attacks and those types of things.

I will conclude with those remarks. Thanks.

● (1145)

[*Translation*]

Mr. Rémi Massé: Thank you.

Mr. Michael Peirce: I'll start and then I'll turn the floor over to my colleague.

[*English*]

Protecting information is part of our core business. Every piece of information that we collect, that we retain, is reported into a specific data bank. Those data banks have limited access, so that they are not available to individuals throughout the organization. Again, this is similar to what Ms. Beck referred to. It's the need-to-know principle that governs, and we have strong restrictions on the access to that information within the service.

We train our people from day one in how to manage information that they collect. When you enter the service, particularly as an intelligence officer, you undergo a course of training before you ever begin to work, so that you know how to collect, manage, and report information, and report it into the right area. We track all of the information that's reported. We have systems that allow us to call it up quickly, particularly because we may need that information in an urgent situation with respect to national security. It also facilitates our ability to respond to privacy requests, which is one of the reasons why we have such a high response rate within the allotted times.

Besides that, we have an ethic of compliance within the organization that leads us to ensure that our people are constantly retrained on how to do this work, how to make sure that they're reporting it in the right place, and that we're protecting the information and that it can't be inadvertently disclosed, both because we have to protect personal information and because we have to protect national security.

The Chair: We're already at eight minutes in the seven-minute question, but I do want to give Citizenship and Immigration a chance. Just be as succinct as you can, please.

Ms. Stefanie Beck: I could just say what they said, because, in fact, I think we all approach it the same way. There are really three major aspects: the personnel side, the physical side, and the IT side. We have similar structures in place on the prevention and detection and the auditing to make sure that it doesn't happen in the first place, but that if it does happen, that we catch it quickly and we deal with it.

The Chair: Thank you very much.

We'll now move to Mr. Kelly for up to seven minutes.

Mr. Pat Kelly (Calgary Rocky Ridge, CPC): This is my first question. I'd like to start with Mr. Peirce.

Are you concerned that any of the Privacy Commissioner's recommendations would impede CSIS in performing its duties, and if so, which ones would? Are there particular recommendations that you might struggle with as an organization in fulfilling your mandate?

Mr. Michael Peirce: I've come here today to talk about the administration of the Privacy Act, as opposed to those policy developments that may take place, so I don't have a particular response to the recommendations.

Mr. Pat Kelly: Okay. Our committee, though, is here to make a recommendation or to address the recommendations that have been made. We would welcome any recommendations that you might have or any concerns that you might have about the recommendations that have been made. If we don't have the opportunity to hear that here, it will impede our ability to produce a report that is necessary on this file.

Mr. Michael Peirce: I'd certainly be pleased to follow up with the committee with a response, but, as I said, I undertook to come here today to testify on how we actually handle and administer the act currently, as opposed to policy pieces. If I'm mistaken in that understanding, then, as I said, we'll follow up with you.

Mr. Pat Kelly: I may offer a few comments if you permit me.

The Chair: By all means.

A/Commr Joe Oliver: Creation of an explicit necessity requirement for collection, I think, would have to be carefully carried out so as not to interfere with evidence gathering if that recommendation is accepted. When it comes to evidence gathering, we pursue evidence where it exists, whether it's travel information, banking information, information on communications, video surveillance, or other types of things. Limiting law enforcement to collect only certain pieces of information could restrict our ability to deliver our public safety mandate.

The other one is with respect to granting the Privacy Commissioner discretion to publicly report on government privacy issues when doing so would be in the public interest. I hope that if that recommendation is adopted, it won't weaken section 62, which relates to the security requirements, or section 65, which relates to the protection of sensitive capabilities, such as investigative techniques, and those types of things.

These are some areas, possibly impeding our ability to deliver our mandate, in which disclosure of certain information could compromise the identity of human sources or the identity of people in witness protection. It could compromise sensitive investigative techniques that we try to protect so that criminal organizations or terrorists do not modify their behaviours to avoid detection or put in place countermeasures to avoid those things. We'd be looking to maintain the protection of that type of information.

● (1150)

Mr. Pat Kelly: Thank you.

Perhaps I'll broaden the question and then allow each of the other two organizations to respond as to whether or not there are specifics.

Ms. Beck, you mentioned in your remarks the concern about the resources for compliance if the Privacy Act is to be extended to foreign nationals, if you'd like to expand on that, please go ahead.

Ms. Stefanie Beck: I think that one is fairly self-evident. When I say we're processing 2.8 million applications annually, if even 10% of those people started to make requests for all of their case files, we would have an enormous amount of work to do.

To add to what my colleague from the RCMP said, we too were curious as to what he meant by reporting on issues in the public interest. More information on that would be useful before we could come to some kind of formal view on it.

The one we are also interested in, of course, is the order-making powers that the Privacy Commissioner is asking for, following what the Information Commissioner has been requesting recently. Similarly, our concern would be where the order-making powers would override what's already in the Privacy Act and what's in the Access to Information Act. We would want to make sure that, notwithstanding new powers given to the commissioner, we could still protect our national security issues. Releasing information about a private individual could cause their family to be put in danger. I'm thinking, for instance, of cases with regard to refugee claims. It would be important that the Privacy Commissioner be aware of all the consequences of the kinds of things that would happen if the information were released, and that would be a major concern for us.

Mr. Pat Kelly: Thank you.

The Chair: Is there anything from the folks at CBSA?

Mr. Robert Mundie: There's nothing on the recommendations of the Privacy Commissioner that we had specific concerns with, but there is one issue we've been grappling with internally, and it may be applicable to the RCMP and Correctional Services.

There are situations under section 8(2) of the Privacy Act in which we can release personal information in a circumstance, but there's also the situation of people having undergone serious injury or death, meaning you can't get their permission to release information to next of kin or family members. That may be an amendment that would serve a purpose, as opposed to having to go through an E2M, which is a way of determining whether the public interest exceeds the personal to release that information, and it's a time-consuming process. In adding an amendment that would be specific to a situation of death or serious injury, we would be in a position to notify next of kin.

Mr. Pat Kelly: Maybe I'll finish again with Mr. Peirce then.

If you have concerns about the 15 recommendations we have, will you respond to those afterwards, so that we have that information from you as a summary?

Mr. Michael Peirce: We'll follow up.

Mr. Pat Kelly: Is that my time?

The Chair: Yes it is.

Mr. Pat Kelly: All right. We'll leave it at that, then.

The Chair: Thank you, Mr. Peirce.

I'm sorry, Mr. Kelly. I didn't mean to interrupt.

Mr. Peirce, by all means, if you have some information, please follow up with the clerk of the committee here and we'll disseminate that information.

We will now move to Mr. Blaikie for up to seven minutes.

Mr. Daniel Blaikie (Elmwood—Transcona, NDP): Thank you all for coming. Because it's a bit of a challenge to have four departments all in one session, I'm going to start with a couple of questions I hope can be answered quite quickly, with a yes or a no, and then I'll get into a more detailed question.

Are there instances in your current operations in which personal information is shared without being covered by an explicit information-sharing agreement, either with another government department or with a foreign government?

● (1155)

Ms. Stefanie Beck: No.

A voice: No.

A/Commr Joe Oliver: No. When we share information, it's for consistent use and it would include caveats regarding further dissemination.

Mr. Daniel Blaikie: In those cases, for all of your departments, would those be written information-sharing agreements? Does any information sharing that occurs happen under the authority of a written agreement with another department or another government?

Mr. Robert Mundie: I could respond.

In the case of another government, foreign or domestic, there will always be a collaborative written arrangement in place, so it is in writing. I believe that with respect to information sharing between government departments, it depends on the circumstances as to whether we have something in writing that's specific. We often rely on the authorities of different acts to do the information exchange. It doesn't necessarily require a written agreement.

A/Commr Joe Oliver: That would be consistent with the situation for the RCMP. As long as it's collected for a consistent use, the disclosure is consistent with the Privacy Act, and we've assessed reliability, relevance, and so forth, then we would share in the absence of agreements, but with caveats attached to that information.

Mr. Michael Peirce: Not all of our agreements with international partners are written agreements. Some of them are oral agreements. They are all documented as being agreements under the provisions of our act, however.

Ms. Stefanie Beck: We have both agreements under our act, the Immigration and Refugee Protection Act, as well as formal written agreements on information sharing. In fact, a lot of those are online, and you can read them on our website.

Mr. Daniel Blaikie: How possible do you think it is, or how easy would it be for you to move from those instances where you don't have formal written agreements, either with other governments or with other departments, to a system where you are always operating under the auspices of a written information-sharing agreement?

Ms. Stefanie Beck: From a bureaucratic perspective, it's always easier if we have legislative authority to do it without having to negotiate a whole separate agreement, if that's what you're suggesting, in order to operate. If we had to write information-sharing agreements among all of us, there are guidelines, drafts, formats, and things like that we could do, but it would seem to me, in an era of red-tape reduction, that is not the direction we would want to take.

Mr. Daniel Blaikie: A suggestion we have heard from some witnesses is that information sharing should always occur under an explicit written agreement, and furthermore, that those agreements should be made public. This is where I'm going next in terms of trying to have a sense both of the operational impact of putting those agreements in place and of what it would mean for your particular organizations to make public the general principles or rules according to which that information is shared—although not the information itself, obviously. What would be the operational impact?

Ms. Stefanie Beck: The acts are all public, and they are online. As I said, about 50 of ours are already online, and we're reviewing to see which others we could put up. The documentation itself isn't classified in any way. There may be parts of it in some instances. You can even read our information-sharing agreements with the U.K. and the U.S. They're up on our website.

Mr. Michael Peirce: Naturally it would be difficult for CSIS to publicize its relationships with all of the security intelligence agencies around the world with whom we work. That would disclose relationships that are closely guarded by some of our partners at times, relationships that may prove problematic to our ability to gather national security information from them about threats to the security of Canada.

Simply put, some organizations would not work with us if they had to publicize that relationship.

Mr. Daniel Blaikie: In your case, then, one of the challenges wouldn't just be the type of information that's being shared and having that disclosed publicly. It would also be the fact of the relationship itself.

● (1200)

Mr. Michael Peirce: That's correct.

Mr. Daniel Blaikie: Okay.

A/Commr Joe Oliver: Where we have long-standing relationships whereby the information is regularly shared, normally that is supported by an agreement that outlines the information protections required. However, it would be operationally impossible, I think, to negotiate an agreement with everybody we share with. If you look at the North American context, you have 360 law enforcement agencies in Canada and 17,000 in the United States. Where the offence takes place may have international implications. For us to share maybe a small portion of information with a state police in the United States, we would have to go through an onerous negotiation process for the sharing of information that is relevant to law enforcement. In some instances, this information has to be shared in a timely manner in order to prevent a more serious crime from taking place.

It would be very challenging to negotiate an agreement with everybody we share with. That's why we have strict policies that dictate how we share and with whom we share. There's a need to know and there's a right to know. Plus, we assess the relevancy of any request, the reliability of the information we are sharing, and the accuracy of that information before we share it. Then it's shared with the caveat that for any further dissemination, you would have to come back to the originator in order to share onward.

Ms. Rennie Marcoux: There's also the ongoing training of our employees so that they understand exactly what their responsibilities are—i.e., to share information or not.

The Chair: The folks at CBSA, I think, have been waiting patiently as well.

Mr. Dan Proulx: At CBSA we have policies that cover basically all possible legislative authorities for disclosure. We have a policy, for example, under section 107 of the Customs Act. We have a policy under the Privacy Act, section 8. We have a policy under SCISA. Granted, there might not be written agreements for every exchange of information, but there's policy governance to assist with those disclosures.

Now, our concern, if you will, is that you would try to implement a written agreement for all consistent-use disclosures. As you know, the Privacy Act is subject to other acts of Parliament that already have governing disclosure provisions, so in terms of consistent use, to have a written agreement for every single one would be very problematic.

Apart from that, when it's not a consistent use, we would agree, and support, that you need a governing framework, an authority, written and signed, to share that information.

The Chair: Thank you very much, Mr. Blaikie. We went past seven minutes there.

We now move to Mr. Lightbound for our last seven-minute round.

Mr. Joël Lightbound (Louis-Hébert, Lib.): First of all, thank you all for being with us today and for the work you do.

My first question is regarding privacy impact assessments. The commissioner in one of his recommendations suggested that all institutions, before implementing a new program, would conduct a privacy impact assessment. We learned this fall that of the 17 institutions that are provided for in SCISA, only two conducted privacy impact assessments.

I'd like to know the frequency with which you conduct privacy impact assessments. I'll start with CBSA.

Mr. Robert Mundie: I think it would probably be better for Dan to answer the question on frequency. I think in our last report we did seven or eight in the course of the year...?

Mr. Dan Proulx: At CBSA we do have a lot of privacy impact assessments under development. If I had to guesstimate, I would say we probably have 40 of them on the go right at the present time. We commonly do privacy impact assessments. We do an assessment of the need for privacy impact assessments.

In terms of how we built in the process at CBSA, we start off with what's called a "privacy impact questionnaire". Basically, that questionnaire is an assessment that is done, based on a review by my office and legal services, to determine if the new program or activity, or the substantive change to the program or activity, requires the development of a new privacy impact assessment. If it does, that privacy impact questionnaire basically serves as chapter one of the PIA. We have a regular review, at a director general level, of all proposed and new PIAs being developed. That is chaired by my director general, Robert Mundie. We have regular follow-ups with the program areas to make sure they're done.

We do have a lot, yes.

● (1205)

Mr. Joël Lightbound: And we do understand that making PIAs mandatory would not be too much of a hassle, considering—

Mr. Dan Proulx: No, it would not. Granted, they're challenging and resource-intensive to put together, because they require a certain level of expertise, which you do not have normally in-house either within an ATIP office or within the agency or the program area. That is a challenge we need to look into.

Mr. Joël Lightbound: Does the RCMP have anything to add?

Ms. Rennie Marcoux: Thank you.

Like CBSA, the RCMP does conduct privacy impact assessments for any new programs or any programs that are substantially amended. Last year, for 2015-16, we completed three privacy impact assessments, and provided three addenda to previously submitted privacy impact assessments. They're listed and explained in depth in our annual report to Parliament.

Mr. Joël Lightbound: Mr. Peirce.

Mr. Michael Peirce: We're in the same situation. We conduct our privacy assessments. We work with the Office of the Privacy Commissioner in doing so, to make sure that they're effective at providing the information necessary.

Ms. Stefanie Beck: The same, as I said in our opening remarks, and in fact we've recently revised our PIA templates and guidelines for the officers writing them. I will say they are lengthy and time-consuming. It's not a simple effort. Even if we're doing, say, seven or eight a year, they can be telephone books, these things.

Mr. Joël Lightbound: We've heard from previous witnesses, for instance, that in B.C. there are requirements to protect or maintain data that is about Canadians in Canada, but there is no similar disposition in the federal law. I was wondering what measures you take to protect the data that pertains to Canadians that is stored outside of Canada, if you have any? Or is it all stored here in Canada, on servers here?

Ms. Stefanie Beck: Shared Services Canada is responsible, of course, but in fact I thought the same did apply to federal data. Certainly when we're undertaking procurement for systems that will have data about Canadians on them, we specify that the servers need to be in Canada.

Mr. Joël Lightbound: Okay.

Ms. Stefanie Beck: I would just add that our missions abroad are deemed to be in Canada. For a Canadian embassy in Costa Rica, the servers that are in that mission are deemed to be in Canada.

Mr. Joël Lightbound: I don't know if anyone has anything to add on this.

I'll go to my next question. I think Mr. Kelly touched upon it. We have heard from a lot of witnesses who suggest that a necessity test would be appropriate. I would like to hear more about the impact that a necessity test for the collection of personal information would have on your various agencies, instead of what is currently in section 4 of the Privacy Act, which relates directly.

Again, we can start with CBSA.

Mr. Dan Proulx: It's a good question.

On a necessity test, I would say that the principle is already embedded in what we do every day. We don't collect information which we have no legal authority to collect. And we don't use it for a purpose for which we should not be using it.

A necessity test, in theory, seems to be a good idea; in practice, I'm not sure how you would apply it, especially with the vast amount of information that we all collect to fulfill our mandates.

Whatever the test, if ever it were embedded in legislation, would have to be operationally feasible, because you have to be able to collect information in real time. I don't know how that would also affect past collection, when the legislation is introduced. Would you have to go back and do a necessity test, or prove that you do indeed have a need to collect that information, or would it start when the new legislation is implemented? There are a lot of unknowns.

My main preoccupation would be for operational reasons. How do you practically implement that and make it work?

Mr. Joël Lightbound: Mr. Oliver.

A/Commr Joe Oliver: Much of our collection is actually judicially authorized. We've presented cases to a judge indicating a compelling reason for us to pursue very specific targeted and focused information under warrant or under production order.

I would say, and I go back to the point that I raised earlier, that if this section were supported, how it would be crafted would be important to us. As I mentioned earlier, we pursue evidence wherever the evidence exists, whether that is DNA, a breath sample, a hair fibre, travel information, financial information, or video surveillance. To create a prescriptive list may limit our ability to deliver our mandate.

If we can demonstrate necessity and show that it's important in the context of proving the elements of an offence in a criminal prosecution, I think that would be the necessity test for us by linking it back to reducing crime, preventing crime, and prosecuting offences. Again, it depends on the evidence that's available, and we would chase the evidence.

● (1210)

The Chair: Thank you very much, Mr. Oliver and Mr. Lightbound.

That ends our seven-minute round.

We're now going to proceed to five-minute sessions for questions and answers. Mr. Jeneroux is going to start us off.

Mr. Matt Jeneroux (Edmonton Riverbend, CPC): Wonderful.

Thank you all for being here and for taking time out of your obviously busy schedules to spend with us, and thanks to all your staff who helped prepare a lot of this as well.

I want to follow up on Mr. Lightbound's initial line of questioning on the privacy impact assessments.

I'm curious about whether, through some of these impact assessments, any of the negative results that have come back have impacted any policy or program that they are, I guess, assessing.

Whoever wants to start may go ahead.

Ms. Stefanie Beck: I think what is most useful in that process, which includes a necessity test, by the way, for a privacy impact assessment—a "necessity of collection" is part of it. In our conversations with, for instance, the Office of the Privacy Commissioner, when we explain what a new program is going to look like, I can recall that in one circumstance they asked why we would expect to retain the documentation for such a long period of time.

In that particular circumstance, we were talking about citizenship. To determine citizenship, we often have to go back several generations. We had to explain why we retain data on file for 150 years, in some cases.

It's that kind of back-and-forth that gives clarity to them and gives us pause, frankly. It makes us think for a moment about whether we really need to retain it, or whether, while it was a circumstance that was necessary 20 years ago that, for some other reason, we can change now because, for instance, of new technology that would enable us to trace in a different way.

Yes, it is a useful process.

Mr. Michael Peirce: I can confirm that response. It is a productive relationship with the Office of the Privacy Commissioner. In doing impact assessments, that back-and-forth is very constructive for us in identifying issues that we need to address. There may be issues with which, when they are seen from a different angle, from the Privacy Commissioner's angle, we can understand there's a challenge and then decide that we should fix it and address it.

It's the back-and-forth, by and large, that's the most productive thing.

Mr. Matt Jeneroux: Just quickly, you can confirm, then, that it has assisted in developing certain policies or procedures?

Mr. Michael Peirce: Absolutely.

Could I very quickly just respond to a previous question, because I didn't have the opportunity to address it. It's the question of necessity.

We already have a necessity test in our act. Section 12 of our act says:

> (1) The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary...

and it goes on to say that this is for the purposes of national security.

So that strict necessity test is already built into our legislation. We wouldn't in that respect have the same transition problems that others may have.

The Chair: We'll resume, then, with your time, Mr. Jeneroux.

We'll hear from the RCMP.

Ms. Rennie Marcoux: Perhaps I could just answer quickly by referring to one of the programs for which we did a privacy impact assessment. It's listed in our annual report. It's called the Identity Insight program. It's software that enables the real-time analysis of operational data from multiple sources. It has helped, over time, as is stated there, to "facilitate the research, analysis... to enhance the de-confliction of person entities".

In other words, I think it has helped to clarify the association, the individual, and their identity. I would say, then, that it has improved our ability to make sure we have the right person.

Mr. Dan Proulx: In regard to privacy impact assessments, we really appreciate the interactions we have with the Office of the Privacy Commissioner. We have regular dealings with them.

We like to engage them early in the development of a privacy impact assessment to get their ideas and to see what they think about how we should go ahead with our program or activity.

Any time we do a PIA at CBSA, we do what's called an action plan. The action plan basically identifies certain levels of deficiencies in the program or activity, and we work with the OPC to come up with solutions to address those.

The recommendations that they give to the agency will have an impact on the delivery of the program. I have not, in my experience, seen one actually stop the delivery of a program or activity, but definitely they have made changes to how we conduct our business.

● (1215)

Mr. Matt Jeneroux: Terrific.

I have about 30 seconds. Is that correct, Chair?

The Chair: Yes. I'll be liberal with you, sir.

Mr. Matt Jeneroux: I appreciate that—small L.

Ms. Beck or Ms. White, you didn't indicate your percentages of compliance. Do you have your compliance rate?

Ms. Stefanie Beck: It's sixty-nine per cent within 30 days, 27% in 31 to 60 days, and the balance, in excess of 60 days, would be about 4% of our 15,292 requests.

Mr. Matt Jeneroux: Right. It's safe to say, then, that the foreign nationals piece has you worried about reaching that existing 69% that you have now. You're worried that it may drop lower.

Ms. Stefanie Beck: Some of those, of course, would be transformed, if I can describe it this way, from ATI requests into P, notwithstanding, I think, that with the 2.8 million, and the fact that it's free, and you could do it online from anywhere.... I don't know that we would see a corresponding drop on the access side.

Mr. Matt Jeneroux: I'm out of time, but I would just like to let the rest of you know that I will be coming back with a question on that to you in the next round of questioning.

The Chair: Okay, thank you very much.

Mr. Saini, go ahead, please.

Mr. Raj Saini (Kitchener Centre, Lib.): Thank you very much, all of you, for being here.

It's very interesting, and it's unfortunate that we have only two hours. I think we could have easily spent two days asking you all the questions.

One question I want to ask is a question I have asked of other agencies, but I think it's more pertinent with the agencies that you represent, because each one of you deals internationally. This question picks up on the question that Mr. Blaikie brought up about international sharing agreements.

Mr. Oliver, you quite rightly pointed out that it's very difficult to have an agreement with every single entity in a different country. For the other agencies, I think it's a little bit easier because they're dealing with one entity, but when you deal with another jurisdiction, there might be multiple layers of different agencies that you have to deal with.

When you are dealing with another country that you have a written sharing agreement with, what confidence do each of you have that the information that you share is confidential and that there's a robust regime or a repository as strong as ours to make sure that information is confidential, especially when you're dealing with a Canadian citizen?

The second question is, if you have a written sharing agreement with one entity or one jurisdiction, there may be another country that has a separate deal with them that we don't have. What guarantee do we have that the information that we have given to one country, with whom we have a written sharing agreement with, does not get passed on to another country, with whom that country may have an agreement?

A/Commr Joe Oliver: From my experience, we put in place the arrangements with them based on guiding principles, and there are guiding principles when it comes to international sharing. We're guided by the ministerial directive in a couple of areas. One is that for any arrangement we have, we must receive advice from Global Affairs, if it's an international arrangement, and legal advice. Global Affairs would have insight and visibility into some of the political dynamics that the RCMP may not have. As we are negotiating, we take that advice and incorporate that into the agreement as well.

When it comes to sharing with national security entities that are international, we also have a ministerial directive on the arrangements that we can enter into with those, and in fact, it limits the number of entities that we can have those arrangements with. But when it comes to compliance—now I can't say in all instances, but in some instances—there are arrangements put in place whereby you can do, not necessarily auditing, but kind of compliance verifications. Of course, if there are instances of a breach of the trust or a breach of the agreement, we can terminate that arrangement as well.

● (1220)

Mr. Raj Saini: If we can use the Five Eyes as an example, you have one partner, England, the U.K., which probably is integrated with a European intelligence network. You have Australia, which may be integrated with a South Pacific network. It may not be done in a way that is meant to injure, but it may be done because they have to share information with the political geography they're in. That's kind of my question. It's awkward, because you're giving information within the practice of making sure that you share intelligence information, but they may have a requirement to share that information with the political geography they're in.

A/Commr Joe Oliver: Let me just qualify a bit in terms of the RCMP's information-sharing arrangements. Our information sharing is strictly related to criminal investigations, so for law enforcement purposes. We don't share national security intelligence with international partners. That's the role of our colleagues in the service. They perform that function.

When it comes to us sharing, it's on a need-to-know basis with those who have a right to know, and it is specifically limited and focused to a law enforcement objective, either for the receiving jurisdiction, or for Canada receiving information, or for the RCMP, so that we can advance a criminal investigation. It's not as if there is broad information sharing that is not controlled.

Mr. Raj Saini: Mr. Peirce, I'm—

Mr. Michael Peirce: Do I get a response to that particular question?

Mr. Raj Saini: Yes, I'm very excited to hear your response.

Mr. Michael Peirce: We have 300 foreign relationships with 150-odd countries. When we enter into a relationship, that must be submitted to the Minister of Public Safety for approval, and that approval will also require consultation with the Minister of Foreign Affairs.

When we enter into a relationship, we will do so on an incremental basis, to test the trust in the relationship. We take slow steps, and we require all institutions, all foreign partners, that we enter into a relationship with, to respect the third-party rule. If we provide information to them, it is not for onward dissemination beyond that organization. If we were to find out that in fact information had been shared beyond that organization, that would compromise our relationship with that organization.

Mr. Raj Saini: What happens if—

The Chair: Before we go any further, Mr. Saini, we're past five minutes.

Is this a quick question?

Mr. Raj Saini: None of my questions are really quick.

The Chair: Can we come back to you at the end, then, Mr. Saini?

Mr. Raj Saini: Sure.

The Chair: Thank you very much.

I'll move to Mr. Jeneroux.

Go ahead, please.

Mr. Matt Jeneroux: Thank you, Mr. Chair.

Going back to my question on foreign nationals, I'm curious about the impact with the other three departments, if you don't mind weighing in on that particular recommendation from your end.

Ms. Rennie Marcoux: I would think we would have the same concerns with regard to the implications of opening both the Privacy Act—and I know it's not the mandate—and the Access to Information Act to foreign nationals, just with regard to our ability to comply with the legislation, and, I suspect as well, to confirm that the person making the request is actually the person whose personal information we would or wouldn't share.

Mr. Matt Jeneroux: Okay.

Anybody else?

Mr. Robert Mundie: It's hard to estimate what kind of volume you would get if you opened it up to people outside of Canada.

Certainly anything that adds to our workload and causes us issues, such as Rennie was mentioning—when we want to validate who the person asking for the information is—makes our life more complicated.

Mr. Michael Peirce: We would face the same challenges.

Mr. Matt Jeneroux: I'll turn it over to my colleague Mr. Kelly.

Mr. Pat Kelly: Thank you.

Could I maybe have a quick comment from each agency on one of the recommendations made by the Privacy Commissioner, the legislation for mandatory breach reporting? I'm wondering about the potential for compounding the damage of a breach against a person by reporting the breach. Perhaps I could have a quick comment from each on current practice and what this recommendation might mean to your organization.

● (1225)

Mr. Dan Proulx: I can go ahead.

At CBSA, we have in place a robust privacy breach protocol, and it's aligned with Treasury Board standards. Any new requirements would be aligned with our breach protocol as well.

All employees are trained to use the breach protocol, and there is a direct linkage with the departmental security officer. As you all know, a privacy breach, for example, is first and foremost a security incident, so everything is reported to a centralized office, which is a departmental security office. If it involves personal information, then the privacy breach protocol is triggered. Any material privacy breach that involves personal information right now is reported to the Office of the Privacy Commissioner. That is a new requirement.

Any change in legislation obviously would require adjustment, but at CBSA we're not expecting that making breach reporting mandatory to the Privacy Commissioner will be problematic at all.

Mr. Pat Kelly: I'll maybe cut you short there just to give each one a chance since we're have limited time. Thanks.

Ms. Rennie Marcoux: I would add that we follow exactly the same process as our colleagues from CBSA do, including having a close relationship with our departmental security officer. They're usually reported in as security breaches.

The concern we would have is with the mandatory reporting of all privacy breaches. Now we actually assess the damage, and when there's material damage we will report it to the Privacy Commissioner and Treasury Board. We do that on a regular basis.

I can give you an example where it would be perhaps not deemed necessary to report a privacy breach, if you wish.

Mr. Pat Kelly: Mr. Peirce.

Mr. Michael Peirce: We have a robust regime for reporting on compliance. That regime operates within the service more broadly and includes reporting to the minister, but also we will work with the Office of the Privacy Commissioner and report privacy breaches specifically.

Again, we don't have a large number of those situations that arise currently, so I don't see a particular issue for us in terms of volume.

Ms. Stefanie Beck: It's the same. Of the thousands that we processed last year, we had 55 material privacy breaches. They were all reported to the OPC and to Treasury Board Secretariat, but also the individuals were notified by letter.

If the mandatory reporting meant that we had to provide all of the same private information to the commissioner, then it would, in effect, constitute another privacy breach. We wouldn't be keen on that, but what we do now is an event summary, basically. That's fine.

The Chair: We have Mr. Bratina for up to five minutes.

Mr. Bob Bratina (Hamilton East—Stoney Creek, Lib.): First of all, Mr. Mundie, I was curious to know whether you thought a wall would be a useful thing to build along the border and how much it might cost, but I'll leave that for later.

Mr. Robert Mundie: All right. Thank you.

Mr. Bob Bratina: Is there a typical kind of complaint? You get this great number of complaints and only 88 were filed against you or the Privacy Commissioner. Can you give me an idea of the nature of the complaints that you deal with?

Mr. Robert Mundie: I know that Dan Proulx can give the answer to that one much better than I can.

Mr. Bob Bratina: Okay.

Mr. Robert Mundie: There's a range of reasons. Dan can elaborate.

Mr. Dan Proulx: Yes. The most common complaint that we have today is delay. With the increase in requests that we have, trying to respond to some 11,000 privacy requests a year, the obvious complaint and the number one complaint is time delay. We're taking too much time to get back to the requester.

That said, our time compliance in 2015-16 was pretty good. It was around 88%, but a handful of people still want it to be faster and they file delay complaints.

The other common complaints are obviously against exemptions invoked. If we protect information from disclosure, people want to know why or they challenge our decisions.

The other type of complaint we get is not strictly about processing an ATIP request, if you will. It is about use and disclosure complaints, when people think that the CBSA misused their information. That's another type of complaint that is also common to receive.

Mr. Bob Bratina: Thanks. That's helpful.

Mr. Peirce, you stated that a number of personal information banks are unique to CSIS, including investigational records and security assessments and advice. How is the data in these banks accessed remotely? Is it a secure flow? Wherever that data is held, how do agents access that data in a secure manner?

● (1230)

Mr. Michael Peirce: Access to those systems is always in a secure environment, and we require certification of the environment in which access will be provided. We have to be in effectively a SCIF situation to receive access to a database.

Mr. Bob Bratina: To our friends from the RCMP, data collected in the field has to move through some sort of chain to get to a secure place. Is that part of the educational nature of what you were talking about earlier in speaking to 750 divisions across Canada about how to deal with that? Is that something you're concerned about and you want to assure is done properly?

A/Commr Joe Oliver: Absolutely. Again I'll go back to the safeguards that are put in place. One of the biggest threats of privacy breaches or information leaks is actually the insider threat. We spend a lot of time with respect to security, screening individuals, and making sure that the right people have access to the right information, and that they are screened at the right level. When it comes to access to RCMP information systems, we actually, in each, have two-factor authentications, so the individual has a password plus a physical token or a key in order to access the data system. Then, the security architecture ensures that it meets certain security requirements, based on the type of information being held. Most of our information is held at the protected A or protected B levels. Then when it gets into national security we will have our classified environment where the security controls are enhanced.

Mr. Bob Bratina: Ms. Beck, on the notion of foreign nationals, those outside Canada can obtain access by hiring a Canadian representative and filing a request. That's how it's done now. The recommendation was that foreign nationals should be able to submit a request, but you're saying it would just be too cumbersome. The complaint we have is that these agents sometimes rip off people who are making legitimate attempts to become Canadian citizens or who have other issues.

Do you have any thoughts about how that system could be improved?

Ms. Stefanie Beck: I guess that's really more of a comment about the access to information legislation rather than about privacy. Is the solution to give them the option to apply under privacy and then it's free, or is the solution to amend the legislation on access to information? For instance, the fee structure is different, or there are different approaches, whether you're making an access to information request as a business or as an individual.

Mr. Bob Bratina: We hear that resources are often a problem in all of the matters that we're discussing.

Ms. Stefanie Beck: Yes, and I would just reiterate that we are trying to put—remember we talked about it last time—more information up online so people can go in and access their own cases. The more we can do that, the easier it will be.

The Chair: Mr. Blaikie, go ahead for our final official round of questioning.

Then I have Mr. Saini, myself, and Mr. Long on the list. That should use up the rest of the hour.

Mr. Blaikie.

Mr. Daniel Blaikie: I think this question is more for Mr. Peirce and Mr. Oliver.

You guys are in an industry where technology is changing a lot, and you obviously have to keep on top of those technological changes in order to be able to do the job well. One of the issues that has come up in the study of the Privacy Act, because it is from 1983 and hasn't been changed for a long time, is that it is not particularly well adapted to new technology.

Do you have any advice for us on how to recommend that the legislation be changed, not just so that it fits the technology as it is right now, but so that it's a law that continues to apply in the next five years or 10 years when the technological landscape is going to be quite different in a way that it doesn't become cumbersome and challenging for your own operations?

Mr. Michael Peirce: I don't have an answer that's going to solve all the problems for the next five years or so as technology evolves. Certainly, though, the broad principles set out in the act are very important for guiding us. We live up to the purpose of the act and not just the specific provisions of the act. We should be enunciating principles and perhaps even modifying the principles going forward in a way that ensures there is a clear idea as technology evolves and touches privacy in different ways. Our practices ought to evolve in the same way with the guidance that we would follow.

● (1235)

A/Commr Joe Oliver: I would support the remarks of my colleagues, but I would also, in relation to one specific recommendation, create a legal obligation with government institutions to safeguard personal information. In the age of information technology, we need to be very mindful of the cyber-threats that exist, and we need to put in place the necessary IT security infrastructure in order to protect that information.

I will also say with respect to this recommendation that the approach to safeguard should be risk-based. I say that because some of the security control measures. If they were consistently applied, and if the measures that are put in place by my colleagues at CSIS were then applied to other government information, the costs would be huge. We need to take a measured approach for risk-based safeguards, based on the type of information being held and based on the threats that exit against that information. Then we must put in place measured security controls that will be cost-effective, but also meet the objective of protecting the information.

Mr. Daniel Blaikie: Thank you.

Would anyone from the other departments want to weigh in on that, or is that a good enough answer?

Ms. Stefanie Beck: Good luck with that.

I didn't know, but you're recommending or somebody is recommending a review every five years. That will help, rather than every 30 years, to keep it broad and big-picture and to give us wiggle room. We like that too.

The Chair: Reviewing it every five years hasn't been a problem. I think getting something changed every five years has been.

We have about 24 or 25 minutes left.

Colleagues, I'll try to keep it around five minutes for the extra time. If you need it, that's fine, but don't feel you have to take it. We haven't heard from Mr. Long yet either. I try to let every member here....

Mr. McLeod, I know you're visiting and sitting in, but if you have something that you'd like to ask, then by all means feel free to participate.

We'll now move to you, Mr. Saini, to finish your line of questioning.

Mr. Raj Saini: I just want to follow up on a point you raised, Mr. Peirce, on the sharing agreements with other countries. You said they were very specific. If data is shared with another country and that country feels that data of an impending threat must be shared, how does that work? Is there a protocol to inform us that they will be doing this? Do they do it before they share that information, is it done after, or is it not done at all?

I recognize that you have certain protocols in place to make sure that this is contained within the sharing agreement with another jurisdiction, but it may be that this jurisdiction, for whatever purposes in its own political geography, may need to share it with someone else. Is there a mechanism whereby they would inform the department that this information is about to be shared and these are the reasons for it, to seek your permission, or to tell you after?

Mr. Michael Peirce: In normal circumstances, an organization that determines that it would be useful and necessary to share information will come back to us and ask our consent to do so. In those circumstances we may work with them. We may say we'll share the information, because we can share it in a slightly different context. We may want to put additional controls on it, and those kinds of discussions will take place.

There's always a possibility of imminent threat, and in an imminent threat situation we'll respond very quickly and provide the approval to use the information as necessary. We have very good communications with our partners that facilitate that kind of timely response in situations where there is imminent threat.

Mr. Raj Saini: This is just a general question to all of you. When you're developing a policy, do you seek the advice of the Privacy Commissioner at the outset, in the middle, or at the end? Do you have that kind of relationship, just so there's an alignment in what you're trying to do to make sure that it meets the goals of the Privacy Commissioner's office also? Could you give me an idea of how that works?

Mr. Dan Proulx: We try to do that at the beginning, especially for policy development work. Early engagement is always the best, based on our experience. They have a lot of good ideas, information, and experience to share, so if you can start your deliberations with the Privacy Commissioner at the beginning of your policy development, we think it is an asset, and you go from there.

To touch a bit on the question that you asked before, and this one as well, regarding the CBSA's written collaborative arrangement you were asking about, and the sharing of information either with levels of government or with international entities, for example, we always define specific elements of personal information to be shared. We always define a specific purpose of the sharing in our working collaborative arrangements. We limit the secondary use and onward transfer of our information, and we outline other measures to be prescribed by regulations, such as specific safeguards, retention, and accountability measures. In all of our purposes for information-sharing, there are always caveats regarding each disclosure that prohibit the activities, or the ongoing sharing of information, unless it's permitted by law or they obtain our permission to do so. Another way to make sure things are done the right way is through audit and redress as well.

Once you build the agreement and it's signed by the two parties, there should be no exceptions to the rules, because it's a signed understanding between two governments or two countries. Apart from audit, I guess you would not know if everyone is respecting their side of the agreement, but they're all in writing for us, when you're talking about agreements with other entities or international partners that are not covered in the consistent use provision that we talked about earlier.

● (1240)

The Chair: Are you satisfied, Mr. Saini?

Mr. Raj Saini: I wanted to ask the RCMP.

Ms. Rennie Marcoux: The RCMP does have a very co-operative, collaborative, and constructive relationship with the Office of the Privacy Commissioner. We don't necessarily consult them at the beginning of a draft policy that's in the works, but doing so would be in our interest as the policy starts to take shape, and we start identifying privacy implications. Then we do reach out and get their advice, for sure.

Ms. Stefanie Beck: We wouldn't do it at the beginning, not at the twinkle-in-the-eye portion, but when we have something a little more substantive we can exchange on, we do.

Mr. Michael Peirce: Early engagement is the principle. What constitutes early engagement? As my colleagues have said, it's an art to determine that now is the time to go. It's in our interests to work with them and to ensure that they understand what we're trying to achieve and to get their guidance in trying to achieve it.

The Chair: Thanks, Mr. Saini.

If colleagues will permit me, I have a few questions myself.

Obviously, Canada is member of Interpol. My question is for those of you who might want to talk about this.

This continues from your line of responses, Mr. Oliver.

Back in the spring, based on some of the attacks that had been happening in Europe, Interpol had a conference. At that conference the Secretary General, who was Jürgen Stock, suggested specifically that “police at the local level must be able to access information shared by local and national police forces across the world.... And law enforcement agencies need to start sharing more of that information, so that a global information network can be 'uncompromisingly and fully [utilized]' by local and national police.” According to Stock, “To be fit for purpose, our response must also be global”. This was the theme of that particular conference.

Now, the Privacy Commissioner has a number of recommendations that have been made so we can update the Privacy Act. The Privacy Commissioner has also been quite vocal about some of the concerns that he has with some of the anti-terrorism legislation that we've had here in Canada in the past.

There seem to be competing interests—this is not a secret—between, obviously, the concern that the citizenry has for the proper and respectful treatment of their private and confidential information and the fact that citizens at large want to know that they can go to bed safely at night, knowing that those who are charged with the responsibility of keeping us safe have the information they need in order to do that.

My question to any of the folks who are here is, do you see any concerns with some of the recommendations that the Information Commissioner is proposing? Do we need to do more as a country to carry our weight when it comes to sharing of information with organizations through Interpol and the like, in order to keep Canadians safe? What assurances can you give me, as a person who makes the decisions from time to time on public policy, that citizens in my riding, for example, and in all ridings across this country can be assured that their personal and private information in the hands of the government is not going to be compromised?

That's a very broad question, but I want to get the Interpol perspective.

Mr. Oliver, I think you're most suited to proceed in answering this question.

● (1245)

A/Commr Joe Oliver: Interpol is an organization of more than 180 members. There are information-sharing arrangements put in place when it comes to specific information. Those are based on agreements. There is a structure around how that information is shared. What I could say is that sharing your information is never taken lightly. It's always considered in the context of the relevancy, the accuracy, the need to know, the right to know, and all of those things, which is consistent with the principles that we live by in Canada—and with our values, of course.

But I can't emphasize enough the importance of the right time for information to be shared quickly and efficiently, as exemplified by the case in Strathroy, Ontario, in which information was received in the early hours of the morning. It was then shared with local law enforcement agencies. That prevented a terrorist attack from happening in Canada.

Those types of things show us the value of sharing information in an efficient and effectively managed situation, with the understanding that it be done responsibly and with the appropriate caveats and so forth.

The Chair: Okay.

Does anyone else want to weigh in on this?

Mr. Michael Peirce: I would say that you articulated the balance that is there. It's a challenge that we live with every day in our work. We certainly strive to share information in a proportionate way. It is, in some respects, even more complex than just the dynamic that you've suggested, because in sharing information we have to be mindful of the individual's interests, the personal information being shared, for instance. We also have to look at the impact of our capacity to continue to investigate. In situations where we have threat-related information, we have to consider whether sharing in that situation is required to counter the threat, and what the impact will be on the investigation itself. Is there a risk of disclosure of a human source in sharing the information? Is there a risk of disclosure of a technical source in sharing the information?

It's a very complex matrix in making that call. That said, certainly, in any circumstances where there is a risk of imminent harm—the Strathroy example is an outstanding one—we will act quickly to share that information with our police colleagues, to ensure that preventative action can be taken.

The Chair: Thank you very much.

We'll now go to Mr. Long, please.

Mr. Wayne Long (Saint John—Rothesay, Lib.): Thank you, Chair.

Thank you to all the presenters today. You've been very informative.

Mr. Mundie, one thing I want to get from you, if you will, is about a case involving Alain Philippon, who was charged for not turning over his cellphone. I just wonder if you could give me some input on that. He was charged. He turned over his cellphone but wouldn't give the password, and then he was subsequently charged. It was settled. There was a $500 fine. I think he pleaded guilty. There might have been an opportunity missed to explore that. It's an emerging legal question, so I just want to get your input on that privacy aspect. Maybe I could get input from the other panellists, too, with respect to cellphones, and passwords, and things like that. It happened in Halifax.

Mr. Robert Mundie: Yes. I'm somewhat familiar. I don't know all of the details of that particular case, but it's under the Customs Act that officers have the right to access the goods that someone possesses. It's the interpretation of what is a good. A cellphone is a good, and its contents were considered a good for review.

What is often found, in terms of child pornography cases, is what's found on hardware. The issue is the consent that the individual is providing to access that information. It is an outstanding legal question, and we're getting some jurisprudence from it as a result of cases such as this.

Mr. Wayne Long: Would anybody else like to weigh in on that one?

A/Commr Joe Oliver: Technology has actually improved the lives of Canadians, and we've adopted technology more quickly than most nations. We spend the most time online. But with the advancements in technology also come opportunities for criminals and terrorists who can use that technology as well.

Investigating crime in the digital age is particularly challenging for law enforcement when it comes to our ability to collect evidence, and there are a number of barriers: whether we have the ability to intercept certain types of information, the use of advanced encryption when we know that evidence exists, the lack of data-retention standards in Canada, things like the Cloud, and the fact that evidence may be stored outside of Canada's jurisdiction.

Even with judicial authorization, even when we've gone to a judge and convinced a judge that we believe that evidence exists at a specific location, and we convince a judge that we have the authority to go search, we are impeded by things like encryption. In fact, one of the biggest barriers to advancing investigations in the digital age is encryption.

I'm not against encryption, because to me encryption is the same idea as police advising people to lock their doors and protect their belongings. But when it comes to the public's expectation of policing, if someone is actually committing a crime in a certain dwelling or in a building, and there's information that the crime exists or there's evidence of that, there's an expectation from the public that we would go in, and get that evidence, and pursue the investigation. In the current digital environment, we are severely encumbered by the inability for us to get past encryption.

In fact, it's recognized even by the Canadian Association of Chiefs of Police. This is not just a question of encryption in national security cases; it's a question of fraud, identity theft, and it's seen throughout the policing community. One of the resolutions that was passed by the Canadian Association of Chiefs of Police called on the federal government to enact some sort of legislation that would give police the authority to go to a judge and seek an order that would compel someone to give their password.

In the context of law enforcement, we don't have an authority, such as CBSA has in the border zone, which the court has recognized as a unique environment. We have to seek authority and judicial authorization to obtain certain authorities to compel the production of information. While it's controversial, it's one of the most significant barriers we're confronted with today. I think the response will have to be measured and transparent, and it will have to include things like safeguarding rights, and accountability when it comes to police using some sort of coercive powers, if that's the direction the government so chooses to go.

● (1250)

Mr. Wayne Long: Does anybody else have a comment?

Thank you.

The Chair: All right. Thank you, Mr. Long.

Colleagues, I've just been reminded that we do have about five minutes of committee business to do, so I'll turn it over to Mr. Kelly to wrap it up and leave us with about five minutes.

Can everybody stay two to three minutes longer. Is that okay? It's very minor committee business.

Mr. Kelly, go ahead and ask your questions, but understand that, as soon as I'm done with Mr. Kelly, I'll be thanking the witnesses and I'll be moving us in camera to do a quick meeting on committee business.

Mr. Lightbound.

Mr. Joël Lightbound: Also I have a very quick submission.

The Chair: Certainly.

Mr. Kelly, quickly, and then Mr. Lightbound.

Mr. Pat Kelly: I will ask Mr. Peirce in particular, and maybe Mr. Oliver might want to weigh in.

In your introduction you reminded the committee, or pointed out, that yours is not an enforcement agency, that you gather information but do not enforce, lay charges, or make arrests. The usefulness of your organization depends on your ability to share information with enforcement agencies. Advocates for privacy raise concerns that sharing of information between departments is perhaps a point for breach, or that an originating organization may lose control of information. Yet you must share information to be able to protect Canadians. Can you describe the sharing-of-information relationship, perhaps in particular with the RCMP, and how the need to share information is important to your organization?

Mr. Michael Peirce: Thank you for your question. You're absolutely right in your description of it. Our ability to share information is fundamental to our mandate, and describing the relationship with the RCMP is a useful way of exploring it.

Certainly I can say unequivocally that the relationship with the RCMP has never been better. We work extremely closely together. The way we work together operates within, quite frankly, a difficult legal environment because it is a challenge to protect our information when we do share it, and it's very important to us to be able to protect that information for our ongoing investigative purposes.

When we share information with the RCMP, we do it according to an agreed-upon structure called the one vision process. That process ensures that we can sit down with the RCMP regularly and share strategically first of all. So here's the overall picture in regard to a threat, and we can discuss at that level who is going to take the lead on it, who is going to manage it, and how. In some circumstances when we do that, the RCMP will say to us, “We would like a disclosure letter from you that simply discloses the fact of the threat” and that can be used then to launch an investigation by the RCMP.

In some circumstances, the RCMP may not be in a position to investigate to the level that we're currently investigating, so for instance, if we have human sources next to the target of investigation, the RCMP may not be in a position to get up and running as quickly as necessary, and we'll have to share information beyond the mere disclosure of the threat. In so doing, we'll share it in the form of an advisory letter with the RCMP to give them additional information that allows them to, for instance, potentially go and get a part VI warrant under the Criminal Code to intercept communications and facilitate that.

All of those discussions that we have with the RCMP are then documented in a record of decision that says, “This is what we discussed in regard to the case. This is the action that's going to be taken in regard to it”, and then the two organizations will continue on.

At any given time, if an issue arises, we are able to reconstitute the meeting and discuss further the strategic approach to it. That allows us to protect our information to the greatest extent possible. There still will be situations, particularly of imminent threat, in which we have to respond quickly and have to provide the necessary information, and in those circumstances, we may be called upon to disclose investigative information that may actually put at risk our investigation. But, in the face of imminent harm, we'll take that step.

● (1255)

The Chair: Mr. Lightbound, go ahead quickly.

Mr. Joël Lightbound: My question is for Mr. Peirce as well. I'd like to know how much of the information that fuels your investigations is gathered by your agency, CSIS, as opposed to shared with you by CSEC.

Mr. Michael Peirce: I couldn't untangle in terms of numbers the exact proportion of information. I can say that we work extremely closely with CSEC and that we have aligned our priorities so that we can work in a collaborative way to be as effective as possible. There's no question that significant information collected by CSEC is very important to our investigations, particularly our overseas investigations, in relation to, for example, foreign fighters, and we will rely on CSEC's capacity to operate internationally to provide that kind of information to us.

We work closely. We have regular meetings with CSEC to align those operational priorities. We do what's called HUMINT enabled SIGINT and SIGINT enabled HUMINT, that is, we rely on their collection to facilitate our investigation, and they will rely on our collection to facilitate their investigation. That proves particularly productive and is something that has really evolved in the last five years or so to a very strong level of co-operation.

The Chair: Thank you very much to the witnesses who appeared before the committee today. Most of you are no strangers to appearing before the committee. Thank you very much for your clear and concise answers. If we need any follow-up or supplemental information, we will be requesting that.

Mr. Peirce, we will be looking forward to an analysis brief on the proposed changes and their effect on CSIS.

I am going to suspend the meeting and ask folks who are not members of Parliament.... If you think you shouldn't be here, chances are you shouldn't. We are going to move in camera, so I would ask that the room be cleared very quickly.

Thank you.

[*Proceedings continue in camera*]